Allegato A

REGOLAMENTO DELL'AUTORITÀ DI REGOLAZIONE PER ENERGIA RETI E AMBIENTE, RELATIVO AGLI ADEMPIMENTI IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI, AI SENSI DELL'ARTICOLO 29 DEL REGOLAMENTO (UE) N. 2016/679 E DELL'ARTICOLO 2-*QUATERDECIES* DEL DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196

Titolo I
Disposizioni generali

Articolo 1
Oggetto, finalità e definizioni

1. Il presente regolamento (di seguito anche: Regolamento o Regolamento Privacy) disciplina, in attuazione del Regolamento (UE) n. 2016/679 (di seguito: GDPR) e del d.lgs. n. 196/2003 (di seguito: Codice Privacy), lo svolgimento dei trattamenti di dati personali da parte dell'Autorità di Regolazione per Energia Reti e Ambiente (di seguito anche: Titolare o ARERA) eseguiti dal personale tutto, al fine di garantire il rispetto dei diritti, delle libertà fondamentali, nonché della dignità di quanti hanno rapporti con l'ARERA, con particolare riferimento alla riservatezza e all'identità personale degli interessati, siano essi interni o esterni alla stessa.
2. Ai fini del Regolamento Privacy vengono assunte le definizioni contenute nel GDPR, nel Codice Privacy, nel d.lgs. n. 82/2005, nel Regolamento di organizzazione e funzionamento di cui alla deliberazione 201/2023/A, che devono intendersi qui integralmente richiamate e per quanto non ivi previsto si intende per:
   a) "Designati di primo livello": il Segretario Generale e i Direttori di Divisione;
   b) "Designati di secondo livello": i Direttori di Direzioni e Responsabili Uffici speciali;
   c) "personale" o "dipendenti": i dipendenti dell'Autorità a tempo indeterminato e a tempo determinato, pieno o parziale, anche in regime di aspettativa, comando, distacco o fuori ruolo, nonché coloro che prestano servizio presso la medesima in posizione di comando, distacco o fuori ruolo da pubbliche amministrazioni o da altri enti pubblici o privati, nonché i dipendenti applicati a qualsiasi titolo da altre amministrazioni pubbliche e gli assegnisti di ricerca per le attività a supporto degli uffici;
   d) "incidente di sicurezza": evento che causa una violazione dei criteri di sicurezza di un'organizzazione e mette i dati a rischio di esposizione, ma che non sempre comporta una violazione di dati personali;
   e) "violazione di dati personali" o "*data breach*": la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati da ARERA e da propri contitolari o responsabili del trattamento, ivi inclusi eventuali sub-responsabili.

Articolo 2
Principi del trattamento

1. I dati personali sono:
   a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
   b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità («limitazione della finalità»);
   c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
   d) esatti e, se necessario, aggiornati, nonché cancellati o rettificati tempestivamente se inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
   e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati, tenuto conto degli obblighi in materia di conservazione degli atti amministrativi e dei documenti pubblici («limitazione della conservazione»);
   f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
2. Il Titolare adotta tutte le misure tecniche e organizzative al fine di assicurare il rispetto dei principi di cui al primo comma del presente articolo («responsabilizzazione»).

Articolo 3
Informativa all'interessato

1. L'informativa è uno dei presupposti di liceità del trattamento dei dati in quanto garantisce l'evidenza e la trasparenza delle attività di trattamento che vengono poste in essere.
2. L'informativa è sempre dovuta, a prescindere dalla base giuridica del trattamento e dall'eventuale obbligo di acquisizione del consenso dell'interessato.

Titolo II
Organizzazione interna di ARERA

Articolo 4
Autorizzazione ai dipendenti al trattamento dei dati personali

1. Ai sensi dell'articolo 29 del GDPR e dell'articolo 2-*quaterdecies* del Codice Privacy, il personale di ARERA è autorizzato al trattamento dei dati relativi alle attività di competenza della unità organizzativa di assegnazione e alle eventuali ulteriori attività attribuite.
2. Il personale autorizzato al trattamento è coordinato dal Designato di riferimento secondo le modalità di cui agli articoli 5 e 6.
3. Il personale è tenuto a rispettare il presente Regolamento, le istruzioni e le procedure impartite da ARERA sul corretto trattamento dei dati personali di cui all'Allegato 1 e quelle adottate ai sensi dell'articolo 18. Tutti i citati atti sono espressamente comunicati al personale al momento della presa di servizio e integrano i doveri d'ufficio.

4. La violazione degli obblighi di cui al comma 3 può comportare l'irrogazione di sanzioni nel rispetto dei principi, delle forme e della regolamentazione interna in materia disciplinare. L'avvio del procedimento sanzionatorio è sempre dovuto qualora dalla violazione degli obblighi di cui al comma 3 consegua l'adozione di un provvedimento sanzionatorio da parte dell'Autorità Garante per la protezione dei dati personali.

Articolo 5
Attribuzioni di funzioni e compiti ai Designati di primo livello

1. Ai sensi dell'articolo 29 del GDPR e dell'articolo 2-*quaterdecies* del Codice Privacy, il Segretario Generale e i Direttori di Divisione sono nominati "Designati di primo livello" e in tale ruolo sono tenuti a svolgere i compiti e le funzioni di seguito indicati:
   a) coordinamento del personale posto alle dirette dipendenze degli stessi, autorizzato ai sensi dell'articolo 4;
   b) coordinamento delle attività svolte dai Designati di secondo livello di cui all'articolo 6;
   c) coinvolgimento tempestivo e adeguato del RPD in tutte le questioni riguardanti la protezione dei dati personali anche tramite la richiesta di pareri su specifiche questioni e tematiche;
   d) acquisizione, per conoscenza, delle comunicazioni inviate al RPD dai Designati di secondo livello relative all'avvio di un nuovo trattamento o a modifiche apportate a trattamenti già svolti, anche tramite applicativo all'uopo predisposto;
   e) predisposizione, in caso di raccolta diretta dei dati dagli interessati, dell'informativa di cui all'articolo 13 del GDPR, che, previa valutazione positiva del RPD, deve essere fornita all'interessato al momento della raccolta dei dati;
   f) predisposizione, in caso di raccolta dei dati presso soggetto diverso dall'interessato, dell'informativa di cui all'articolo 14 del GDPR, che, previa valutazione positiva del RPD, deve essere fornita all'interessato entro un termine ragionevole dall'ottenimento dei dati personali;
   g) conoscenza delle informative relative ai trattamenti che sono svolti, anche al fine di rendere, ove richiesto dall'interessato, l'informativa oralmente;
   h) collaborazione con il RPD nella predisposizione dei riscontri alle istanze di esercizio dei diritti degli interessati nei termini di cui all'articolo 11 del Regolamento Privacy;
   i) predisposizione degli accordi di contitolarità del trattamento di cui all'articolo 26 del GDPR o acquisizione dai Designati di secondo livello delle richieste di sottoscrizione degli stessi e, previa acquisizione del positivo parere del RPD, sottoscrizione degli stessi;
   j) predisposizione degli accordi di nomina di responsabili del trattamento di cui all'articolo 28 del GDPR e sottoscrizione degli stessi, previa acquisizione del positivo parere del RPD circa l'adozione, da parte dei responsabili, di adeguate misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio insito nel trattamento che gli stessi saranno chiamati a svolgere;
   k) coordinamento della procedura di notifica delle violazioni di dati personali di competenza ai sensi degli articoli 12 e seguenti del Regolamento Privacy e invio al Garante, previa intesa con il RPD, delle notifiche e cura delle successive interlocuzioni;
   l) valutazione, con il supporto del RPD, rispetto ai nuovi trattamenti e a quelli già svolti, cui sono apportate modifiche sostanziali, della necessità di svolgimento della valutazione d'impatto sul trattamento di dati di cui all'articolo 35 del GDPR e, in caso

di risposta positiva, avvio della procedura valutativa con la partecipazione necessaria del Designato di secondo livello interessato e l'acquisizione obbligatoria del parere del RPD;

m) svolgimento, ove necessario, della procedura di consultazione preventiva di cui all'articolo 36 del GDPR, richiedendo obbligatoriamente il parere del RPD;
n) valutazione, sentito il Direttore della Direzione Legale, della possibilità di presentare un esposto o denuncia, anche contro ignoti, all'autorità giudiziaria in caso di attività penalmente rilevanti, quali attacchi cibernetici, sospetta attività fraudolenta o altri casi di sospetto illecito;
o) acquisizione, per conoscenza, delle istanze presentate dagli interessati per l'esercizio dei diritti di cui agli articoli da 15 a 22 del GDPR;
p) acquisizione del censimento dei fabbisogni formativi in materia di trattamento dei dati dei dipendenti effettuato dai Designati di secondo livello e invio al RPD e alla Direzione Affari Generali e Risorse del fabbisogno formativo complessivo entro il 30 giugno di ciascun anno;
q) sottoscrizione di tutti gli atti conseguenti allo svolgimento dei compiti sopra riportati, inclusi gli accordi di contitolarità e di nomina dei responsabili del trattamento che devono essere trasmessi per archiviazione al RPD.

2. I testi di accordi di contitolarità e di nomina dei responsabili devono espressamente recare la dichiarazione da parte dei contraenti di conoscenza e accettazione integrale del presente Regolamento.
3. Nello svolgimento delle attività i Designati di primo livello sono tenuti a osservare, oltre alle istruzioni di cui all'Allegato 1, anche quelle riportate nell'Allegato 2 al presente Regolamento.
4. I Designati di primo livello possono indicare il nominativo di uno o più funzionari cui è attribuito il ruolo di "Referente *privacy*" che li assistono nella gestione degli adempimenti di cui al presente articolo. Ai Referenti *privacy* sono attribuiti i compiti di cui all'articolo 7. I nominativi dei Referenti *privacy* sono comunicati al RPD che cura la pubblicazione dell'elenco completo sul sito *intranet*.

Articolo 6
Attribuzioni di funzioni e compiti ai Designati di secondo livello

1. Ai sensi dell'articolo 29 del GDPR e dell'articolo 2-*quaterdecies* del Codice Privacy, i Direttori di Direzioni e i Responsabili di Uffici speciali sono nominati "Designati di secondo livello" e in tale veste ad essi sono attribuiti, per i trattamenti di dati personali svolti nell'ambito della Direzione o Ufficio speciale di riferimento, i seguenti compiti e funzioni:
   a) coordinamento del personale autorizzato ai sensi dell'articolo 4;
   b) coinvolgimento tempestivo e adeguato del RPD in tutte le questioni riguardanti la protezione dei dati personali anche tramite la richiesta di pareri su specifiche questioni e tematiche;
   c) invio tempestivo al RPD e, per conoscenza, al Designato di primo livello, delle comunicazioni relative alla necessità di censire nuovi trattamenti nel Registro dei trattamenti del Titolare o di apportare modifiche a trattamenti già svolti, anche tramite applicativo all'uopo predisposto;

d) predisposizione e invio al Designato di primo livello, previa acquisizione del parere positivo del RPD, della richiesta di sottoscrizione di accordi di contitolarità del trattamento dei dati, di cui all'articolo 26 del GDPR;
e) predisposizione degli accordi di nomina di responsabili del trattamento di cui all'articolo 28 del GDPR e sottoscrizione degli stessi, previa acquisizione del positivo parere del RPD circa l'adozione, da parte dei responsabili, di adeguate misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio insito nel trattamento che gli stessi saranno chiamati a svolgere;
f) predisposizione, in caso di raccolta diretta dei dati dagli interessati, dell'informativa di cui all'articolo 13 del GDPR, che, previa valutazione positiva del RPD, deve essere fornita all'interessato al momento della raccolta dei dati;
g) predisposizione, in caso di raccolta dei dati presso soggetto diverso dall'interessato, dell'informativa di cui all'articolo 14 del GDPR, che, previa valutazione positiva del RPD, deve essere fornita all'interessato entro un termine ragionevole dall'ottenimento dei dati personali;
h) conoscenza delle informative relative ai trattamenti che sono svolti, anche al fine di rendere, ove richiesto dall'interessato, l'informativa oralmente;
i) collaborazione con il RPD nella predisposizione dei riscontri alle istanze di esercizio dei diritti degli interessati, nei termini di cui all'articolo 11 del Regolamento Privacy;
j) partecipazione alla procedura di valutazione d'impatto dei trattamenti di competenza della Direzione di riferimento;
k) verifica del rispetto da parte degli autorizzati delle istruzioni impartite dal Titolare del trattamento di cui all'Allegato 1 del Regolamento Privacy;
l) rispetto delle procedure di cui al Titolo III;
m) censimento, con cadenza almeno annuale, degli specifici fabbisogni formativi in materia di trattamento dei dati dei dipendenti assegnati alla Direzione, da comunicare al Designato di primo livello, alla Direzione Affari Generali e Risorse e al RPD;
n) sottoscrizione di tutti gli atti conseguenti allo svolgimento dei compiti sopra riportati, inclusi gli accordi di nomina dei responsabili del trattamento che devono essere trasmessi per archiviazione al RPD.

2. Alla luce delle risultanze dell'attività di cui al comma 1, lett. c), del presente articolo, i Designati di secondo livello possono delimitare le autorizzazioni dei dipendenti assegnati alla propria Direzione a specifici trattamenti censiti, dando loro specifiche istruzioni. A tal fine può essere utilizzato il modello A, incluso nell'Allegato 2.
3. I testi di accordi di contitolarità predisposti e di nomina dei responsabili devono espressamente recare la dichiarazione da parte dei contraenti di conoscenza e accettazione integrale del presente Regolamento.
4. I Designati di secondo livello sono tenuti a partecipare attivamente e in prima persona alle iniziative formative loro dedicate.
5. Nell'esecuzione dei compiti di cui al presente articolo, ogni Designato di secondo livello deve coinvolgere il Designato di primo livello e il RPD e attenersi alle loro indicazioni o fornire adeguate motivazioni qualora decida di discostarsene.
6. Nello svolgimento delle attività, i Designati di secondo livello sono tenuti a osservare, oltre alle istruzioni di cui all'Allegato 1, anche quelle riportate nell'Allegato 2 al presente Regolamento.
7. I Designati di secondo livello individuano il nominativo di uno o più funzionari, nella misura minima di un funzionario per Direzione o Ufficio, nella misura massima di un funzionario per Unità, cui è attribuito il ruolo di "*Referente privacy*" che li assistono nella

gestione degli adempimenti di cui al presente articolo. Ai Referenti privacy sono attribuiti i compiti di cui all'articolo 7. I nominativi dei Referenti privacy sono comunicati al RPD, che cura la pubblicazione dell'elenco completo sul sito *intranet*.

Articolo 7
Compiti e funzioni dei Referenti *privacy*

1. Ai Referenti *privacy* sono attribuiti i seguenti compiti e funzioni:
   a) predisposizione delle comunicazioni al RPD relative alla necessità di censire nuovi trattamenti nel Registro dei trattamenti del Titolare o di apportare modifiche a trattamenti già svolti, anche tramite applicativo all'uopo predisposto;
   b) supportare il Designato di riferimento, anche mediante interlocuzioni con il RPD, nella predisposizione delle informative sul trattamento dei dati da rendere agli interessati ai sensi degli articoli 13 e 14 del GDPR;
   c) supportare il Designato di secondo livello, anche mediante interlocuzioni con il RPD, nella predisposizione degli accordi di contitolarità e di nomina dei responsabili del trattamento;
   d) partecipazione alla procedura di valutazione d'impatto dei trattamenti di competenza della Direzione o Unità di riferimento;
   e) partecipazione alle riunioni dei Referenti *privacy* e alle iniziative formative loro dedicate promosse dal RPD.
2. Eventuali ulteriori compiti possono essere attribuiti per iscritto al Referente *privacy* dal Designato di secondo livello, dandone comunicazione al RPD.

Articolo 8
Designazione del Responsabile dell'Unità Servizi Informativi al coordinamento degli amministratori di sistema

1. Al Responsabile dell'Unità Servizi Informativi della Direzione Affari Generali e Risorse (di seguito: Responsabile SIN), sono attribuiti i seguenti compiti e funzioni, secondo quanto prescritto dal Garante per la protezione dei dati personali nel provvedimento del 27 novembre 2008:
   a) nominare gli amministratori di sistema, previa valutazione dell'esperienza, della capacità e dell'affidabilità dei soggetti che si intendono designare, individuando per ciascuno di essi i sistemi di cui viene affidata l'amministrazione;
   b) tenere l'elenco degli amministratori di sistema, ove devono essere riportate le funzioni a ciascuno di essi attribuite, che deve essere pubblicato sul sito *intranet*;
   c) verificare, con cadenza almeno annuale, l'idoneità dei soggetti nominati amministratori di sistema rispetto alle misure di sicurezza, tecniche e organizzative definite, sentiti i Designati di primo e di secondo livello e il RPD;
   d) predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure di sicurezza;
   e) curare la tenuta e l'aggiornamento del registro degli *asset*;
   f) curare la tenuta del registro degli incidenti di sicurezza;
   g) assistere i Designati e il RPD nello svolgimento delle procedure di valutazione d'impatto, anche nella individuazione delle misure di mitigazione del rischio;

h) assistere i Designati di primo e di secondo livello nelle interlocuzioni con il Garante per la protezione dei dati personali e nell'attuazione dei correttivi eventualmente indicati dallo stesso.

2. I soggetti nominati amministratori di sistema sono tenuti a osservare, oltre alle istruzioni di cui all'Allegato 1, anche le istruzioni riportate nell'Allegato 3 al Regolamento Privacy.

Articolo 9
Autorizzazione al trattamento dei dati del Responsabile della prevenzione della corruzione e della trasparenza

1. Ai sensi dell'articolo 29 del GDPR e dell'articolo 2-*quaterdecies* del Codice Privacy, il RPCT, eventuali suoi sostituti, e i dipendenti nominati ausiliari per la gestione delle segnalazioni effettuate ai sensi del Decreto Whistleblowing sono autorizzati a eseguire il trattamento dei dati personali e di altre informazioni riservate riguardanti i soggetti segnalanti (se non anonimi), i soggetti comunque menzionati o coinvolti, gli eventuali facilitatori e i soggetti segnalati.
2. I soggetti autorizzati ai sensi del comma 1, i cui nominativi sono pubblicati nel sito *intranet*, sono tenuti al rispetto oltre alle istruzioni di cui all'Allegato 1, della procedura di cui alla deliberazione 311/2023/A e delle istruzioni specifiche di cui all'Allegato 4 al Regolamento Privacy.

Articolo 10
Compiti e funzioni del Responsabile della protezione dei dati

1. Al RPD sono attribuiti i seguenti compiti e funzioni:
   a) informare, sensibilizzare e fornire consulenza ad ARERA e al personale della stessa, in merito agli obblighi derivanti dalla disciplina europea e nazionale in materia di protezione dei dati;
   b) sorvegliare sull'osservanza del GDPR, del Codice Privacy e dei provvedimenti del Garante per la protezione dei dati personali, nonché delle istruzioni impartite da ARERA in materia di protezione dei dati personali;
   c) valutare l'adeguatezza delle informative redatte ai sensi degli articoli 13 e 14 del GDPR;
   d) coordinare le risposte alle istanze degli interessati, formulate ai sensi degli articoli da 15 a 22 del GDPR e tenere il Registro delle istanze;
   e) rendere i pareri sugli accordi di contitolarità ai sensi dell'articolo 26 del GDPR e di nomina dei responsabili del trattamento ai sensi dell'articolo 28 del GDPR;
   f) conservare gli accordi di contitolarità e di nomina dei responsabili firmati e i relativi registri dei contitolari e dei responsabili di ARERA;
   g) curare i rapporti con i responsabili del trattamento, richiedendo il registro dei trattamenti svolti in qualità di responsabili di ARERA ed esercitare il diritto di controllo e qualsiasi altro diritto di ARERA sugli stessi, previsto negli accordi di nomina;
   h) tenere il Registro dei trattamenti di cui all'articolo 30 del GDPR svolti da ARERA in qualità di titolare e di responsabile del trattamento, raccogliendo le comunicazioni dei Designati di primo e secondo livello, nonché dei responsabili del trattamento, anche per il tramite di applicativo all'uopo dedicato;

i) supportare i Designati di primo e di secondo livello nella procedura per la gestione delle violazioni dei dati personali disciplinata dal Regolamento Privacy;
j) fornire il proprio parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento, ai sensi dell'articolo 35 del GDPR;
k) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per le questioni connesse al trattamento dei dati;
l) aggiornare periodicamente l'analisi dei rischi e verificare se le misure di sicurezza tecniche ed organizzative adottate continuano ad essere adeguate anche avvalendosi dei Referenti *privacy*;
m) collaborare, con approccio operativo, alla definizione del disegno organizzativo interno più idoneo, tenuto conto dell'evoluzione della normativa in materia di trattamento dei dati personali;
n) svolgere periodicamente *audit* interni, al fine di individuare profili di ottimizzazione del rispetto della normativa in materia di trattamento dei dati, suggerendo le potenziali azioni da assumere;
o) effettuare gli *audit* sui responsabili del trattamento, anche avvalendosi, ove previsto, di società esterne allo svolgimento di tale attività espressamente delegate;
p) redigere il piano della formazione in materia di protezione dei dati, da articolare in relazione all'organizzazione del personale e dei trattamenti presso ARERA, tenendo conto dei fabbisogni formativi ricevuti da Designati di primo e secondo livello;
q) erogare la formazione di cui al piano predisposto, avvalendosi anche di professionisti e di professori universitari altamente specializzati nel settore del trattamento dei dati personali;
r) coordinare le attività dei Referenti *privacy* mediante sessioni formative e riunioni di gruppo per il supporto a tutte le attività di cui alle lettere precedenti;
s) curare la pubblicazione dell'elenco completo dei Referenti *privacy* sul sito *intranet*;
t) promuovere e partecipare ad iniziative convegnistiche, progetti di ricerca e a tavoli di confronto con altre autorità indipendenti e pubbliche amministrazioni in materia di trattamento dei dati, al fine di mantenere e accrescere la propria conoscenza specialistica.

2. Al RPD può essere delegata la notifica al Garante per la protezione dei dati personali delle violazioni di dati personali approvata dall'Autorità.
3. Il RPD riferisce direttamente al Collegio dell'Autorità cui presenta annualmente una relazione sulle attività svolte e sullo stato di attuazione della normativa in materia di protezione di dati personali in ARERA.
4. Il RPD è tenuto al segreto e alla riservatezza in merito all'adempimento dei propri compiti e non può essere rimosso o penalizzato per l'adempimento degli stessi.
5. Il RPD è tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali anche tramite la richiesta di pareri su specifiche questioni e tematiche.
6. L'Autorità assicura al RPD, attraverso gli strumenti previsti dal Regolamento di organizzazione e funzionamento, il sostegno e le risorse, anche economiche, necessarie per assolvere i compiti e funzioni previsti dal GDPR, dal Codice Privacy e dal Regolamento Privacy.

Titolo III
Procedure per lo svolgimento di specifiche attività

Articolo 11
Procedura per la gestione delle istanze finalizzate all'esercizio dei diritti degli interessati di cui agli articoli da 15 a 22 del GDPR

1. Le istanze degli interessati provengono prevalentemente, salvo particolari eccezioni, tramite uno dei seguenti canali: *i)* la Divisione o Direzione che detiene i dati; *ii)* lo Sportello per il Consumatore Energia e Ambiente presso Acquirente Unico; *iii)* il RPD; *iv)* un responsabile del trattamento.
2. Nelle ipotesi *sub i)*, *ii)* e *iv)* di cui al precedente comma, la richiesta deve essere trasmessa entro due giorni al RPD, alla casella di posta elettronica rpd@arera.it.
3. Il RPD provvede ad annotare tutte le istanze nel relativo registro entro due giorni lavorativi dalla ricezione e a richiedere una eventuale integrazione documentale o a dichiarare l'istanza inammissibile.
4. Ove necessario per tutelare i dati dell'interessato trattati da ARERA da intromissioni di terzi, il RPD, tenuto conto della tipologia dell'istanza, può procedere preliminarmente a chiedere al soggetto istante un documento comprovante la propria identità. La medesima richiesta è effettuata ove sussistano o emergano ragionevoli dubbi circa tale identità.
5. Annotata la richiesta nel registro delle istanze entro due giorni lavorativi dalla ricezione di cui al comma 3 o dall'identificazione di cui al comma 4 del presente articolo, il RPD, entro i successivi cinque giorni, la indirizza via mail, in base al contenuto, al Designato di riferimento che tratta i dati personali oggetto dell'istanza dell'interessato, fornendo indicazioni di massima sulle attività da svolgersi.
6. Il Designato di riferimento, ove del caso, inoltra l'istanza dell'interessato al responsabile del trattamento o al contitolare del trattamento, fornendo le indicazioni sulle attività da svolgersi e assegnando un termine massimo per la risposta.
7. Il Designato di riferimento completa entro sette giorni le attività di competenza, ivi inclusa l'eventuale interlocuzione con il responsabile del trattamento o con il contitolare del trattamento, e trasmette le risultanze al RPD.
8. Il RPD, entro i successivi sette giorni, fornisce un riscontro all'interessato e annota l'invio della comunicazione nel registro delle istanze.
9. Ai sensi dell'articolo 19 del GDPR, l'istanza di rettifica, cancellazione o limitazione, se accolta, deve essere notificata, per i seguiti di competenza, al responsabile del trattamento o al contitolare del trattamento, cui i dati personali dell'interessato siano stati eventualmente trasmessi.
10. Ai sensi dell'articolo 12, comma 3, del GDPR, il Designato di riferimento, tenuto conto della complessità e della numerosità delle richieste, può chiedere al RPD, entro venticinque giorni dalla ricezione dell'istanza, di comunicare all'interessato, entro i successivi cinque giorni, la proroga di due mesi del termine per fornire le informazioni relative alla gestione dell'istanza dell'interessato.
11. Qualora la richiesta dell'interessato sia manifestamente infondata o eccessiva, in particolare per il suo carattere ripetitivo, il Designato di riferimento e il RPD possono:
    a) richiedere il previo pagamento di un eventuale contributo spese per la sola copertura dei costi amministrativi da sostenere o sostenuti;
    b) rifiutare di soddisfare la richiesta.

12. In base al principio di responsabilità di cui all'articolo 24 del GDPR, la procedura per l'esercizio dei diritti degli interessati deve essere espletata da ciascuno dei soggetti coinvolti nel rispetto del Regolamento.

Articolo 12
Procedura per la gestione delle violazioni dei dati personali

1. La procedura per la gestione delle violazioni dei dati personali è articolata in cinque fasi consecutive distinte, di seguito specificate:
   a) segnalazione della violazione;
   b) analisi della violazione e valutazione del rischio;
   c) notifica al Garante (eventuale);
   d) comunicazione all'interessato (eventuale);
   e) registrazione e analisi finale.

Articolo 13
Segnalazione della violazione

1. Le segnalazioni di violazione possono pervenire:
   a) dal sistema di rilevazione e gestione degli incidenti di sicurezza del SIN;
   b) da autorizzati e designati;
   c) da contitolari del trattamento e da responsabili del trattamento;
   d) da fonti esterne ad ARERA (quali segnalazioni e informazioni pubblicate sulla stampa o sul *web*).
2. Ciascun autorizzato, qualora venga a conoscenza o determini una potenziale violazione di dati, ne informa via mail, immediatamente, il Designato di primo e di secondo livello di riferimento, il RPD, e, se la sospetta violazione coinvolge sistemi informatici, il Responsabile SIN fornendo ogni elemento utile all'analisi degli accadimenti. La segnalazione può essere effettuata compilando e inviando l'Allegato 5 o fornendo le informazioni ivi richieste (data presunta di avvenuta violazione, data e ora in cui si è avuta conoscenza della presunta violazione, fonte della segnalazione, tipologia della violazione, descrizione evento anomalo, presunto numero di interessati coinvolti, quantità e caratteristiche dei dati personali interessati dalla presunta violazione, luogo in cui è avvenuta la violazione dei dati, eventuale descrizione dei *device* e dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione).
3. I contitolari del trattamento, se previsto dall'accordo di cui all'articolo 26, e i responsabili del trattamento, secondo i termini concordati negli accordi di nomina di cui all'articolo 28 del GDPR, se riscontrano una possibile violazione di dati personali informano ARERA immediatamente, e, comunque, entro il termine orario negoziato nei suddetti accordi, decorrente da quando è venuto a conoscenza del fatto.
4. Il RPD annota la segnalazione ricevuta nel Registro delle violazioni dei dati personali e, ove destinatario di comunicazione, il Responsabile SIN annota la segnalazione nel Registro degli incidenti di sicurezza.

Articolo 14
Analisi della violazione e valutazione del rischio

1. Il Designato di primo e di secondo livello referenti delle attività segnalate, con il RPD e, ove interessato, il Responsabile SIN, compongono la "Gruppo di Intervento Data Breach" (di seguito: GIDB) e valutano se l'evento segnalato possa configurarsi come violazione di dati personali sulla base delle informazioni disponibili, eventualmente disponendo, anche con l'ausilio dei contitolari e dei responsabili del trattamento, ulteriori verifiche e approfondimenti.
2. Il Designato di primo livello interessato può richiedere la partecipazione anche del Direttore della Direzione Legale e può integrare la composizione della GIDB di cui al comma 1 del presente articolo.
3. La GIDB, raccolte tutte le informazioni in merito alla violazione, effettua una valutazione di severità del rischio, tenendo conto del tipo di violazione, della natura dei dati personali compromessi, della facilità di identificazione dei soggetti interessati, della potenziale gravità delle conseguenze per gli individui, anche considerando la vulnerabilità delle persone colpite e il numero degli interessati coinvolti.
4. La GIDB assegna un punteggio al rischio, applicando la metodologia di valutazione del rischio ritenuta più idonea dal RPD, tenuto anche conto delle indicazioni e delle linee guida del Garante e del Comitato europeo per la protezione dei dati, e termina le valutazioni di competenza redigendo la Scheda di Valutazione del Rischio di cui all'Allegato 6.
5. Se il rischio è valutato di livello basso, non si procede agli adempimenti di cui all'articolo 16 del Regolamento Privacy e la GIDB valuta se sussistano elementi di opportunità per procedere comunque alla notifica al Garante nei termini di cui all'articolo 15.
6. Se la GIDB valuta che il livello del rischio sia medio, alto o altissimo, si procede alla notifica al Garante ai sensi dell'articolo 15 e, ove sussistano i presupposti, alla comunicazione agli interessati nei termini di cui all'articolo 16.
7. La GIDB, in ogni caso, definisce in qualsiasi momento le attività da intraprendere affinché siano tempestivamente adottate le eventuali opportune misure di contenimento che consentano di minimizzare e mitigare gli effetti conseguenti alla violazione riscontrata e le misure per prevenire il ripetersi di future violazioni.

Articolo 15
Notifica al Garante

1. Il Designato di primo livello competente, con l'assistenza della GIDB, notifica la violazione entro 72 ore dall'avvenuta conoscenza, rilevando a tal fine l'orario indicato nella segnalazione di cui all'articolo 12, tramite il portale predisposto dal Garante per la protezione dei dati personali, dandone tempestiva informazione all'Autorità.
2. Il Designato di primo livello deve essere in grado di giustificare eventuali ritardi nella notifica.
3. La notifica al Garante può essere delegata dal Designato di primo livello competente al RPD o al Designato di secondo livello.

Articolo 16
Comunicazione agli interessati

1. Qualora dalla violazione possa derivare un rischio medio, alto o altissimo per i diritti e le libertà delle persone fisiche, il Designato di primo livello competente, con l'assistenza del RPD, comunica la violazione agli interessati senza ingiustificato ritardo dall'avvenuta conoscenza e valutazione dell'evento, descrivendo con un linguaggio semplice e chiaro la natura della violazione dei dati, attraverso il canale di comunicazione ritenuto più idoneo.
2. L'obbligo di comunicazione all'interessato non sussiste se risulta soddisfatta una delle seguenti condizioni:
   a) sono state messe in atto adeguate misure tecniche e organizzative di protezione e tali misure sono state applicate ai dati personali oggetto della violazione, con particolare riguardo a quelle destinate a limitare l'accesso ai soli soggetti autorizzati, quali, a titolo esemplificativo, la crittografia;
   b) sono state adottate ulteriori misure atte a evitare l'insorgere di un rischio elevato per i diritti e le libertà degli interessati;
   c) la comunicazione richiederebbe per ARERA sforzi sproporzionati.
3. Nell'ipotesi di cui al comma 2, lett. c), del presente articolo il Designato di primo livello competente provvede mediante la pubblicazione nel sito internet di ARERA di una comunicazione, o analoga misura che assicuri un'adeguata possibilità di conoscenza agli interessati.
4. La comunicazione all'interessato deve contenere le seguenti informazioni:
   a) data e ora della violazione, anche solo presunta, e data e ora in cui si è avuta conoscenza della stessa;
   b) natura della violazione dei dati personali;
   c) nome del Titolare e dati di contatto del Titolare e del RPD, presso cui acquisire maggiori informazioni;
   d) gli eventuali rischi derivanti dalla violazione dei dati personali;
   e) una descrizione sintetica delle misure adottate o che si intendono adottare per superare la violazione ovvero per attenuarne i possibili effetti negativi.

Articolo 17
Registrazione e analisi finale

1. Il RPD annota tempestivamente gli eventi, inclusi quelli che siano qualificati con rischio basso e per i quali si decida di non procedere alla notifica, nel Registro delle violazioni dei dati personali di cui all'articolo 14.
2. In sede di analisi finale il RPD, di concerto con i Designati di primo e secondo livello competenti e con il Responsabile SIN, esamina tutte le informazioni e le evidenze acquisite in relazione alla violazione rilevata, nonché alle singole fasi del procedimento di gestione concluso, per verificare l'efficacia delle azioni intraprese e identificare possibili aree di miglioramento.

Articolo 18
Adozione di ulteriori procedure

1. Il Segretario Generale, in veste di designato di primo livello ai sensi dell'articolo 5 del presente Regolamento, è autorizzato ad adottare con propria determinazione, acquisito il parere favorevole del RPD e previa comunicazione all'Autorità, ulteriori procedure per il trattamento dei dati personali.
2. Le procedure adottate ai sensi del comma 1 del presente articolo sono pubblicate sul sito *intranet* di ARERA, comunicate a tutto i dipendenti e notificate ai contitolari e ai responsabili del trattamento, eventualmente anche avvalendosi della collaborazione del RPD.